- 1 -

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	:	Before the Examiner:
David Carroll Challener	:	Nguyen, Nga B.
	:	
Serial No.: 09/851,956	:	Group Art Unit: 3692
	:	
Filing Date: May 9, 2001	:	
	:	
Title: SYSTEM AND METHOD	:	Lenovo (United States) Inc.
FOR INSTALLING A REMOTE	:	Building 675, Mail C-137
CREDIT CARD AUTHORIZATION	:	4401 Silicon Drive
ON A SYSTEM WITH A TCPA	:	Durham, NC 27709
COMPLIANT CHIPSET	:	

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I.   REAL PARTY IN INTEREST

        The real party in interest is Lenovo (Singapore) Pte. Ltd., which is the
assignee of the entire right, title and interest in the above-identified patent application.

II.   RELATED APPEALS AND INTERFERENCES

        There are no other appeals or interferences known to Appellant, Appellant's
legal representative or assignee which will directly affect or be directly affected by or
have a bearing on the Board's decision in the pending appeal.

III.   STATUS OF CLAIMS

        Claims 1-27 are pending in the Application.   Claims 1-27 stand rejected.
Claims 1-27 are appealed.

IV.   STATUS OF AMENDMENTS

Appellant has not submitted any amendments following receipt of the final rejection with a mailing date of October 19, 2006.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1:

In one embodiment of the present invention, a method comprising the step of receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA). Specification, pages 11, line 20 – page 12, line 6; Specification, page 12, lines 7-14; Specification, page 12, lines 15-21; Figure 2, steps 204, 205. The method further comprises creating a public/private key pair and a third certificate in response to the receiving step. Specification, page 13, lines 5-22; Figure 2, step 207. The method further comprises sending the public/private key pair and the third certificate to the customer over the network. Specification, page 13, lines 5-6; Specification, page 14, lines 1-15; Figure 2, step 207.

Independent Claim 7:

In one embodiment of the present invention, a method comprising the step of creating a TPM identity at a customer's computer system. Specification, page 8, lines 14-15; Figure 2, step 201. The method further comprises obtaining, at the customer's computer system, a first certificate from a first server supporting a CA over a network. Specification, page 9, lines 6-15;. The method further comprises creating, at the customer's computer system, a non-migratable key. Specification, page 9, line 19; Specification, page 10, lines 4-5; Figure 2, step 202. The method further comprises transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company. Specification, pages 11, line 20 –

page 12, line 6; Specification, page 12, lines 7-14; Specification, page 12, lines 15-21; Figure 2, steps 204, 205.

Independent Claim 16:

In one embodiment of the present invention, a computer program product adaptable for storage on a computer readable medium, comprising the program step of receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA). Specification, page 7, line 11 – page 8, line 4; Specification, pages 11, line 20 – page 12, line 6; Specification, page 12, lines 7-14; Specification, page 12, lines 15-21; Figure 2, steps 204, 205. The computer program product further comprises the program step of creating a public/private key pair and a third certificate in response to the receiving step. Specification, page 7, line 11 – page 8, line 4; Specification, page 13, lines 5-22; Figure 2, step 207. The computer program product further comprises the program step of sending the public/private key pair and the third certificate to the customer over the network. Specification, page 7, line 11 – page 8, line 4; Specification, page 13, lines 5-6; Specification, page 14, lines 1-15; Figure 2, step 207.

Independent Claim 21:

In one embodiment of the present invention, a computer program product adaptable for storage on a computer readable medium comprising the program step of creating a TPM identity. Specification, page 7, line 11 – page 8, line 4; Specification, page 8, lines 14-15; Figure 2, step 201. The computer program product further comprises the program step of obtaining a first certificate from a CA. Specification, page 7, line 11 – page 8, line 4; Specification, page 9, lines 6-15. The computer program product further comprises the program step of creating a non-migratable key. Specification, page 7, line 11 – page 8, line 4; Specification, page 9, line 19;

Specification, page 10, lines 4-5; Figure 2, step 202. The computer program product further comprises the program step of contacting the web site supporting a credit card company. Specification, page 7, line 11 – page 8, line 4; Specification, page 11, lines 19-20; Figure 2, step 203. The computer program product further comprises the program step of sending to the web site an application for a credit card authorization, the TPM identity, the first certificate, and the non-migratable key. Specification, page 7, line 11 – page 8, line 4; Specification, pages 11, line 20 – page 12, line 6; Specification, page 12, lines 7-14; Specification, page 12, lines 15-21; Figure 2, steps 204, 205. The computer program product further comprises the program step of receiving from the web site a public/private key pair and a second certificate enabling the credit card authorization. Specification, page 7, line 11 – page 8, line 4; Specification, page 13, lines 5-6; Specification, page 14, lines 1-15; Figure 2, step 207.

<u>Independent Claim 25:</u>

In one embodiment of the present invention, a system comprises a server supporting a web site of a credit card company. Specification, page 6, lines 12-18; Figure 3, element 302. The system further comprises a customer computer including a TPM. Specification, page 6, lines 12-18; Specification, page 8, line 14 – page 9, line 2; Figure 3, element 301. The system further comprises a network linked to the server and the customer computer. Specification, page 6, lines 12-14; Figure 3, element 303. The system further comprises first software stored in memory in the customer computer for requesting the TPM to create a TPM identity. Specification, page 6, line 19 – page 7, line 1; Specification, page 7, line 11 – page 8, line 4; Specification, page 8, lines 14-15; Figure 2, step 201. The system further comprises second software stored in memory in the customer computer for obtaining a first certificate over the network from a CA. Specification, page 6, line 19 – page 7, line 1; Specification, page 7, line 11 – page 8, line 4; Specification, page 9, lines 6-15. The system further comprises a third software stored in memory in the customer computer for creating a non-migratable key. Specification, page 6, line 19 – page 7,

4

line 1; Specification, page 7, line 11 – page 8, line 4; Specification, page 9, line 19; Specification, page 10, lines 4-5; Figure 2, step 202. The system further comprises a fourth software stored in memory in the customer computer for browsing the web site of the credit card company over the network. Specification, page 6, line 19 – page 7, line 1; Specification, page 7, line 11 – page 8, line 4; Specification, page 11, lines 19-20; Figure 2, step 203. The system further comprises a fifth software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network. Specification, page 6, line 19 – page 7, line 1; Specification, page 7, line 11 – page 8, line 4; Specification, pages 11, line 20 – page 12, line 6; Figure 2, step 204. The system further comprises a sixth software stored in memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity, the first certificate, and the non-migratable key. Specification, page 6, line 19 – page 7, line 1; Specification, page 7, line 11 – page 8, line 4; Specification, pages 11, line 20 – page 12, line 6; Specification, page 12, lines 7-14; Specification, page 12, lines 15-21; Figure 2, steps 204, 205. The system further comprises the web site of the credit card company creating a public/private key pair and a second certificate. Specification, page 13, lines 5-22; Figure 2, step 207. The system further comprises the web site of the credit card company sending the public/private key pair and the second certificate over the network to the customer computer. Specification, page 13, lines 5-6; Specification, page 14, lines 1-15; Figure 2, step 207.

Independent Claim 26:

A system comprises a memory. Specification, page 6, line 22 – page 7, line 1; Specification, page 7, line 11 – page 8, line 4; Figure 1, element 114. The system further comprises code stored in the memory. Specification, page 7, line 11 – page 8, line 4. The system further comprises an adapter which communicates data to and receives data from a certificate server and a credit card application server. Specification, page 7, lines 3-5; Figure 1, element 134. The system further comprises a Trusted Platform Module (TPM). Specification, page 8, lines 14-21; Figure 1,

element 111. The system additionally comprises a CPU, operatively coupled to the memory, the TPM, and the communications adapter, and which executes code stored in the memory. Specification, page 6, lines 19-20; Figure 1, element 110. The system further comprises the CPU when executing the code effective in creating a TPM identity. Specification, page 7, line 11 – page 8, line 4; Specification, page 8, lines 14-15; Figure 2, step 201. The CPU when executing the code effective in obtaining from the communications adapter a first certificate originating from the certificate server. Specification, page 7, line 11 – page 8, line 4; Specification, page 9, lines 6-15. The CPU when executing the code effective in creating a non-migratable key. Specification, page 7, line 11 – page 8, line 4; Specification, page 9, line 19; Specification, page 10, lines 4-5; Figure 2, step 202. The CPU when executing the code effective in transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate to the credit card application server. Specification, page 7, line 11 – page 8, line 4; Specification, pages 11, line 20 – page 12, line 6; Specification, page 12, lines 7-14; Specification, page 12, lines 15-21; Figure 2, steps 204, 205.

> Independent Claim 27:

In one embodiment of the present invention, an adapter through which data is exchanged with a certificate server and a credit card application server, a Trusted Platform Module (TPM) which creates a TPM identity; a CPU coupled to the adapter and to the TPM and effective in: (1) obtaining from the adapter a first certificate originating from the certificate server. Specification, page 6, lines 19-20; Specification, page 7, lines 3-5; Specification, page 7, line 11 – page 8, line 4; Specification, page 8, lines 14-15; Specification, page 9, lines 6-15; Figure 1, elements 110, 111, 134. The CPU coupled to the adapter and to the TPM and effective in (2) creating a non-migratable key and transferring the non-migratable key, the TPM identity, the first certificate, and a credit card authorization application to the credit card application server. Specification, page 9, lines 19-20; Specification, page 10, lines 4-5; Specification, pages 11, line 20 – page 12, line 6; Specification, page

12, lines 7-14; Specification, page 12, lines 15-21; Figure 1, element 110; Figure 2, steps 202, 204, 205.

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Trusted Computing Performance Alliance (TCPA), TCPA Design Philosophies and Concepts, Version 1.0 (hereinafter "TCPA").

VII.   ARGUMENT

The Examiner has rejected claims 1-27 under 35 U.S.C. §103(a) as being unpatentable over TCPA. Office Action (10/19/2006), page 3. Appellant respectfully traverses these rejections for at least the reasons stated below.

A.   TCPA, taken singly or in combination, does not teach or suggest the following claim limitations.

1.   Claims 1 and 16 are patentable over TCPA.

Appellant respectfully asserts that TCPA does not teach or suggest "receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA)" as recited in claim 1 and similarly in claim 16. The Examiner cites Sections 2.4.1.1; 2.4.1.2 and 2.5.1 of TCPA as teaching the above-cited claim limitations except the limitation of "receiving from a customer over a network an application for a credit card authorization." Office Action (10/19/2006), pages 3-4. Appellant respectfully traverses.

TCPA instead teaches a computing platform involving a subsystem requires the support of a PKI, although a subsystem does not itself explicitly use that PKI. Page 7, Section 2.4.1.1. TCPA additionally teaches that generally, a CA enables determination of the identity by providing a certificate that binds the identity label of

an entity to the cryptographic identity (public key) of that entity. *Id.* Furthermore, TCPA teaches that any certificate that grants an identity to a subsystem must include the statement 'TCPA subsystem identity,' and the signature on the certificate must encompass the statement. Page 7, Section 2.4.1.2. TCPA further teaches that to create a subsystem identity that is recognized by the PKI, the TPM must contain a private endorsement key. Page 9, Section 2.5.1. TCPA further teaches that the owner must make available the endorsement credential, the platform credential, the conformance credential, and the public key of a Privacy CA. *Id.*

Hence, TCPA teaches that a certificate authority provides a certificate that binds the identity label of an entity to the cryptographic identity (public key) of that entity. Further, TCPA teaches that any certificate that grants an identity to a subsystem must include the statement 'TCPA subsystem identity.'

There is no language in the cited passages that teaches receiving from a customer over a network a non-migratable key. Neither is there any language in the cited passages that teaches receiving from a customer a non-migratable key and a first certificate by a TPM identify associated with a computer system used by the customer. Neither is there any language in the cited passages that teaches a second certificate acquired by the computer system from a certification authority.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1 and 16, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant further asserts that TCPA does not teach or suggest "creating a public/private key pair and a third certificate in response to the receiving step" as recited in claim 1 and similarly in claim 16. The Examiner cites Section 2.4.1.7 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 4. Appellant respectfully traverses.

TCPA instead teaches that the 'Trusted Platform Module Entity' (TPME) is the entity that vouches that a TPM is actually a TPM. Page 8, Section 2.4.1.7. TCPA further teaches that the TPME, and only the TPME, provides the root of the trust in the TPM. *Id.*

There is no language in the cited passage that teaches creating a public/private key pair. Neither is there any language in the cited passage that teaches creating a public/private key pair and a third certificate in response to the receiving step.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1 and 16, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant further asserts that TCPA does not teach or suggest "sending the public/private key pair and the third certificate to the customer over the network" as recited in claim 1 and similarly in claim 16. The Examiner cites page 10 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 4. Appellant respectfully traverses and asserts that TCPA instead teaches the three main phases in obtaining evidence of TPM identity. Page 10. There is no language in the cited passage that teaches sending a public/private key pair. Neither is there any language in the cited passage that teaches sending a public/private key pair and a third certificate to a customer. Neither is there any language in the cited passage that teaches sending a public/private key pair and a third certificate to a customer over the network. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1 and 16, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

        2.   <u>Claims 2-6 and 17-20 are patentable over TCPA for at least the reasons that claims 1 and 16, respectively, are patentable over TCPA.</u>

Claims 2-6 each recite combinations of features of independent claim 1, and hence claims 2-6 are patentable over TCPA for at least the above-stated reasons that claim 1 is patentable over TCPA.

Claims 17-20 each recite combinations of features of independent claim 16, and hence claims 17-20 are patentable over TCPA for at least the above-stated reasons that claim 16 is patentable over TCPA.

      3.   Appellant traverses the Examiner's assertion that the missing claim limitation of claims 1 and 16 is well known in the art.

As understood by Appellant, the Examiner asserts that TCPA does not teach "receiving from a customer over a network an application for a credit card authorization" as recited in claim 1 and similarly in claim 16. Office Action (10/19/2006), page 4. The Examiner asserts that receiving from a customer over a network an application for a credit card authorization is well known in the art. *Id.* Appellant respectfully traverses and requests the Examiner to provide a reference that teaches receiving from a customer over a network an application for a credit card authorization pursuant to M.P.E.P. §2144.03. Since the Examiner has not provided any such evidence, but instead, relies upon his own subjective opinion, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1 and 16. M.P.E.P. §2143; *See In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002).

      4.   Examiner's motivation for modifying TCPA to include the missing claim limitation of claims 1 and 16 is insufficient to establish a *prima facie* case of obviousness.

As stated above, as understood by Appellant, the Examiner asserts that TCPA does not teach "receiving from a customer over a network an application for a credit card authorization" as recited in claim 1 and similarly in claim 16. Office Action (10/19/2006), page 4. The Examiner's motivation for modifying TCPA to include the above-cited missing claim limitation is "for the purpose [of] improving the security in purchasing products using credit card over the network." *Id.* The Examiner's

motivation is insufficient to establish a *prima facie* case of obviousness in rejecting claims 1-6 and 16-20.

Most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). That is, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify the reference or to combine reference teachings. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Whether the Examiner relies on an express or an implicit showing, the Examiner must provide particular findings related thereto. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

The Examiner has not provided a source for his motivation for modifying TCPA to include the above-cited missing claim limitation. The Examiner simply states "for the purpose [of] improving the security in purchasing products using credit card over the network" as motivation for modifying TCPA to include the above-cited claim limitation. The motivation to modify TCPA must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-48 (Fed. Cir. 1998). Appellant respectfully requests the Examiner to point out which of these sources is the source of the

Examiner's motivation[1].   The Examiner has not provided any evidence that his motivation comes from any of these sources. Instead, the Examiner is relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 1-6 and 16-20. *Id.*

    Further, the Examiner's motivation ("for the purpose [of] improving the security in purchasing products using credit card over the network") does not provide reasons, as discussed further below, that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify TCPA to include the above-indicated missing claim limitation of claims 1 and 16. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 1-6 and 16-20. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

    TCPA teaches that the TCPA specification contains no normative statements about a TCPA subsystem. Page 1. TCPA further teaches that nothing in the TCPA specification is intended to imply the status of any particular data or method for compliance with the TCPA specification. Page 1. TCPA further teaches that the

---

[1] Appellant feels it is very important for the Examiner to point out the source of the Examiner's motivation because it appears to Appellant that the Examiner is relying upon his own subjective opinion. The reason why the Federal Circuit (*In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2000)) has required the Examiner to provide objective evidence is because it may be easy to conclude that it would be obvious to combine references using hindsight reasoning even though there is no motivation or suggestion to do so. One can usually find a reason to combine references or make modifications to the main reference. If that were all it took, then all inventions would be obvious and not patentable. For example, assuming that a wheelbarrow had never been developed and a patentee had claimed a wheelbarrow, if the main reference taught a cart with a shallow box body, and the secondary reference taught two wheels, then the Examiner could simply assert, using hindsight reasoning without providing objective evidence, that the motivation for combining the two references is so that the cart could be moved from place to place. Hence, the patentee could not obtain a patent on the wheelbarrow (even though one has never been developed) based on the Examiner's rationale for combining the references. Yet the Examiner has not provided any evidence that a person of ordinary skill in the art would have combined the references to make such a product. In hindsight, everything is obvious. It seems that a question that should be asked is why the invention (in this example a wheelbarrow) was not already developed. If it is so obvious, then it would seem it already would have been developed.

purpose of the specification is to encourage the use of computer platforms for critical purposes. Page 1. The Examiner has not provided any reasons as to why one skilled in the art would modify the specification of TCPA (which teaches that it contains no normative statements about a TCPA subsystem and is a specification to encourage the use of computer platforms for critical purposes) to receive from a customer over a network an application for a credit card authorization (missing claim limitation). The Examiner's motivation ("for the purpose [of] improving the security in purchasing products using credit card over the network") does not provide such reasoning.

Why would the reason to modify the specification of TCPA (which teaches that it contains no normative statements about a TCPA subsystem and is a specification to encourage the use of computer platforms for critical purposes) to receive from a customer over a network an application for a credit card authorization (missing claim limitation) be to improve the security in purchasing products using credit card over the network? What is the rationale connection between improving the security in purchasing products via a credit card over the network (Examiner's motivation) and receiving from a customer over a network an application for a credit card authorization (missing claim limitation)? Hence, the Examiner's motivation does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify TCPA to include the missing claim limitation of claims 1 and 16. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 1-6 and 16-20. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

5.   Claims 2 and 17 are patentable over TCPA.

As understood by Appellant, the Examiner asserts that TCPA does not teach "wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network" as recited in claim 2 and similarly in claim 17. Office Action (10/19/2006), page 4. The Examiner

asserts that wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network is well known in the art. *Id.* Appellant respectfully traverses and requests the Examiner to provide a reference that teaches that wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network pursuant to M.P.E.P. §2144.03. Since the Examiner has not provided any such evidence, but instead, relies upon his own subjective opinion, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 2 and 17. M.P.E.P. §2143; *See In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002).

Further, the Examiner's motivation for modifying TCPA to include the above-cited missing claim limitation is "for the purpose [of] improving the security in purchasing products using credit card over the network." *Id.* The Examiner's motivation is insufficient to establish a *prima facie* case of obviousness in rejecting claims 2 and 17.

As stated above, most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). That is, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify the reference or to combine reference

teachings. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Whether the Examiner relies on an express or an implicit showing, the Examiner must provide particular findings related thereto. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

The Examiner has not provided a source for his motivation for modifying TCPA to include the above-cited missing claim limitation. The Examiner simply states "for the purpose [of] improving the security in purchasing products using credit card over the network" as motivation for modifying TCPA to include the above-cited claim limitation. The motivation to modify TCPA must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-48 (Fed. Cir. 1998). Appellant respectfully requests the Examiner to point out which of these sources is the source of the Examiner's motivation. The Examiner has not provided any evidence that his motivation comes from any of these sources. Instead, the Examiner is relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 2 and 17. *Id.*

Furthermore, the Examiner's motivation appears to have been gleaned only from Appellant's disclosure. Any judgment on obviousness must not include knowledge gleaned only from Appellant's disclosure. *In re McLaughlin*, 170 U.S.P.Q. 209, 212 (C.C.P.A. 1971). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 2 and 17. M.P.E.P. §2145.

<p style="text-align:center">6. Claims 3 and 18 are patentable over TCPA.</p>

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the TPM identity is a public/private key pair created as a result of a command by the

customer input into the computer system" as recited in claim 3 and similarly in claim 18. The Examiner cites pages 9-10 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 4. Appellant respectfully traverses.

TCPA instead teaches that to create a subsystem identity that is recognized by the PKI, the TPM must contain a private endorsement key. Page 9, section 2.5.1. TCPA further teaches that the owner must make available the endorsement credential, the platform credential, the conformance credential, and the public key of a privacy CA. Page 9, section 2.5.1. TCPA additionally teaches that the process of obtaining evidence of TPM identity has three main phases. Page 9, section 2.5.1.

There is no language in the cited passages that teaches that the TPM identity is a public/private key pair created as a result of a command. Neither is there any language in the cited passages that teaches that the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 3 and 18, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

7.   Claims 4 and 19 are patentable over TCPA.

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity" as recited in claim 4 and similarly in claim 19. The Examiner cites pages 9-10 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 4. Appellant respectfully traverses.

TCPA instead teaches that to create a subsystem identity that is recognized by the PKI, the TPM must contain a private endorsement key. Page 9, section 2.5.1. TCPA further teaches that the owner must make available the endorsement credential, the platform credential, the conformance credential, and the public key of a privacy

CA. Page 9, section 2.5.1. TCPA additionally teaches that the process of obtaining evidence of TPM identity has three main phases. Page 9, section 2.5.1.

There is no language in the cited passages that teaches that the second certificate is created by the Certification Authority. Neither is there any language in the cited passages that teaches that the second certificate is created by the Certification Authority in response to receiving a third certificate. Neither is there any language in the cited passages that teaches that the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM. Neither is there any language in the cited passages that teaches that the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 4 and 19, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

8.   Claims 5 and 20 are patentable over TCPA.

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the third certificate is associated with an endorsement key of the TPM" as recited in claim 5 and similarly in claim 20. The Examiner cites pages 9-10 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 4. Appellant respectfully traverses.

TCPA instead teaches that to create a subsystem identity that is recognized by the PKI, the TPM must contain a private endorsement key. Page 9, section 2.5.1. TCPA further teaches that the owner must make available the endorsement credential, the platform credential, the conformance credential, and the public key of a privacy CA. Page 9, section 2.5.1. TCPA additionally teaches that the process of obtaining evidence of TPM identity has three main phases. Page 9, section 2.5.1.

There is no language in the cited passages that teaches that the third certificate is associated with an endorsement key. Neither is there any language in the cited passages that teaches that the third certificate is associated with an endorsement key of the TPM. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 5 and 20, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

> 9.   Examiner has not specifically addressed claims 7-15 and 21-24 and therefore has not established a *prima facie* case of obviousness in rejecting claims 7-15 and 21-24.

The Examiner simply states that "claims 7-15 and 21-24 contain similar limitations found in claims 1-6 above, therefore, are rejected by the same rationale[2]." Office Action (10/19/2006), page 5. Appellant respectfully traverses the assertion that claims 7-15 and 21-24 contain limitations that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claims 7-15 and 21-24. In an obviousness rejection, the Examiner is required to provide a reference or combination of references that teaches or suggests each of the claim limitations in order to establish a *prima facie* case of obviousness. M.P.E.P. §§2142-2143. The Examiner has not met this requirement.

Appellant respectfully asserts that TCPA does not teach or suggest "creating a TPM identity at a customer's computer system; obtaining, at the customer's computer

---

[2] Appellant would like to note that the Examiner initially rejected all claims by simply citing pages 1-30 of TCPA in the Examiner's non-final office action. When Appellant requested the Examiner to particularly point out where all the claim limitations were taught, the Examiner issued a final office action addressing only particular claim limitations. Appellant filed a pre-appeal conference request pointing out that the Examiner has not specifically addressed each claim limitation; however, it was to no avail. Hence, Appellant had no choice but to file an appeal brief. Appellant believes it will be unfair for the Examiner to reopen prosecution after all these attempts in having the Examiner address each of the claim limitations. Appellant requests the Examiner's supervisor, Hyung S. Sough, and the other conferee, in the appeal conference to have the Examiner file an Examiner's Answer instead of having the Examiner reopen prosecution citing new art. Appellant has experienced a tremendous amount of delay and expense in other cases by Examiner's consistently reopening prosecution since those on the appeal conference allow the Examiner many opportunities to strengthen their case. This is unfair, a waste of time and a waste of client's monies.

system, a first certificate from a first server supporting a CA over a network; creating, at the customer's computer system, a non-migratable key; and transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company" as recited in claim 7. There are no claim limitations in claim 7 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 7. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 7, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "the second server supporting the credit card company creating a public/private key pair and a second certificate in response to the transferring step; and transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system" as recited in claim 8. There are no claim limitations in claim 8 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 8. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 8, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using a traditional mail service" as recited in claim 9. There are no claim limitations in claim 9 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 9. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 9, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using the network" as recited in claim 10. There are no claim limitations in claim 10 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 10. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 10, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "a customer using the public/private key pair and the second certificate for commercial transactions over the network" as recited in claim 11. There are no claim limitations in claim 11 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 11. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 11, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the creating step further comprises creating a public/private key pair" as recited in claim 13. There are no claim limitations in claim 13 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 13. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 13, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the step of the customer's computer system obtaining the first certificate from the first server supporting the CA over the network further comprises the steps of: transferring from the customer's computer system to the first server supporting the CA a public

portion of the public/private key pair created when the TPM identity is created and a third certificate associated with an endorsement key of the TPM; the CA checking an authenticity of the third certificate; the CA creating a fourth certificate for the TPM identity; the CA encrypting the fourth certificate; the CA bundling the encrypted fourth certificate with the public portion of the public/private key pair created when the TPM identity is created to create a first bundle; and the CA encrypting the first bundle with a public key of the third certificate to create a second bundle" as recited in claim 14. There are no claim limitations in claim 14 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 14. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 14, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "a computer program product adaptable for storage on a computer readable medium, comprising the program steps of: creating a TPM identity; obtaining a first certificate from a CA; creating a non-migratable key; contacting a web site supporting a credit card company; sending to the web site an application for a credit card authorization, the TPM identity, the first certificate, and the non-migratable key; and receiving from the web site a public/private key pair and a second certificate enabling the credit card authorization" as recited in claim 21. There are no claim limitations in claim 21 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 21. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 21, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "conducting a commercial transaction over the Internet using the credit card authorization as enabled by the public/private key pair and the second certificate" as recited in claim 22. There are no claim limitations in claim 22 that are similar to

claims 1-6 such that the Examiner has effectively addressed the limitations of claim 22. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 22, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the non-migratable key is a signing key" as recited in claim 23. There are no claim limitations in claim 23 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 23. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 23, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "wherein the non-migratable key is a storage key" as recited in claim 24. There are no claim limitations in claim 24 that are similar to claims 1-6 such that the Examiner has effectively addressed the limitations of claim 24. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 24, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

> 10.   <u>Claim 25 is patentable over TCPA.</u>
>
>> a.   <u>TCPA does not teach or suggest the following claim limitations.</u>

Appellant respectfully asserts that TCPA does not teach or suggest "third software stored in memory in the customer computer for creating a non-migratable key" as recited in claim 25. The Examiner cites section 2.5.1 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 5. In particular, the Examiner asserts that TCPA's teaching of a private endorsement key is equivalent to the teaching of a non-migratable key. *Id.* Appellant respectfully traverses.

The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that the teaching of a private endorsement key in TCPA is equivalent to creating a non-migratable key. *See Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the teaching of a private endorsement key in TCPA is equivalent to creating a non-migratable key, and that it would be so recognized by persons of ordinary skill. *See In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of obviousness for rejecting claim 25. M.P.E.P. §2143.

Appellant further asserts that TCPA does not teach or suggest "sixth software stored in memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity, the first certificate, and the non-migratable key" as recited in claim 25. The Examiner cites section 2.12.2 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 5. Appellant respectfully traverses.

TCPA instead teaches that each TPM uses a private endorsement key. Section 2.12.2. TCPA further teaches that this key, in conjunction with the endorsement certificate, proves that the TPM is genuine. Section 2.12.2.

There is no language in the cited passage that teaches software stored in the memory in the customer computer for sending to the web site of the credit card company. Neither is there any language in the cited passage that teaches software stored in the memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity. Neither is there any language in the cited passage that teaches software stored in the memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity and the first certificate. Neither is there any language in the cited passage that teaches software stored in the memory in the customer

computer for sending to the web site of the credit card company over the network the TPM identity, the first certificate, and the non-migratable key. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 25, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant further asserts that TCPA does not teach or suggest "the web site of the credit card company creating a public/private key pair and a second certificate" as recited in claim 25. The Examiner cites section 2.4.1.7 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 6. Appellant respectfully traverses.

TCPA instead teaches that the 'Trusted Platform Module Entity' (TPME) is the entity that vouches that a TPM is actually a TPM. Section 2.4.1.7. TCPA further teaches that the TPME, and only the TPME, provides the root of the trust in the TPM. Section 2.4.1.7.

There is no language in the cited passage that teaches a web site of the credit card company. Neither is there any language in the cited passage that teaches a web site of the credit card company creating a public/private key pair. Neither is there any language in the cited passage that teaches a web site of the credit card company creating a public/private key pair and a second certificate. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 25, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant further asserts that TCPA does not teach or suggest "the web site of the credit card company sending the public/private key pair and the second certificate over the network to the customer computer" as recited in claim 25. The Examiner cites page 10 of TCPA as teaching the above-cited claim limitation. Office Action (10/19/2006), page 6. Appellant respectfully traverses.

TCPA instead teaches that the owner creates the identity inside the TPM and then all necessary data is collated inside the TSS. Page 10.

There is no language in the cited passage that teaches a web site of the credit card company. Neither is there any language in the cited passage that teaches a web site of the credit card company sending the public/private key pair. Neither is there any language in the cited passage that teaches a web site of the credit card company sending the public/private key pair and the second certificate. Neither is there any language in the cited passage that teaches a web site of the credit card company sending the public/private key pair and the second certificate over the network to the customer computer. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 25, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

        b.   <u>Appellant traverses the Examiner's assertion that the missing claim limitations of claim 25 are well known in the art.</u>

As understood by Appellant, the Examiner asserts that TCPA does not teach "fifth software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network" as recited in claim 25. Office Action (10/19/2006), page 5. The Examiner asserts that these claim limitations are well known in the art. *Id.* Appellant respectfully traverses and requests the Examiner to provide a reference that teaches these claim limitations pursuant to M.P.E.P. §2144.03. Since the Examiner has not provided any such evidence, but instead, relies upon his own subjective opinion, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 25. M.P.E.P. §2143; *See In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002).

        c.   <u>Examiner's motivation for modifying TCPA to include the missing claim limitations of claim 25 is insufficient to establish a *prima facie* case of obviousness.</u>

As stated above, as understood by Appellant, the Examiner asserts that TCPA does not teach "fourth software stored in memory in the customer computer for browsing the web site of the credit card company over the network; fifth software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network" as recited in claim 25. Office Action (10/19/2006), page 6. The Examiner's motivation for modifying TCPA to include the above-cited missing claim limitation is "for the purpose [of] improving the security in purchasing products using credit card over the network." *Id.* The Examiner's motivation is insufficient to establish a *prima facie* case of obviousness in rejecting claim 25.

As stated above, most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). That is, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify the reference or to combine reference teachings. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Whether the Examiner relies on an express or an implicit showing, the Examiner must provide particular findings related thereto. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

The Examiner has not provided a source for his motivation for modifying TCPA to include the above-cited missing claim limitations. The Examiner simply states "for the purpose [of] improving the security in purchasing products using credit card over the network" as motivation for modifying TCPA to include the above-cited claim limitations. The motivation to modify TCPA must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-48 (Fed. Cir. 1998). Appellant respectfully requests the Examiner to point out which of these sources is the source of the Examiner's motivation. The Examiner has not provided any evidence that his motivation comes from any of these sources. Instead, the Examiner is relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claim 25. *Id.*

Further, the Examiner' motivation ("for the purpose [of] improving the security in purchasing products using credit card over the network") does not provide reasons, as discussed further below, that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify TCPA to include the above-indicated missing claim limitations of claim 25. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claim 25. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

TCPA teaches that the TCPA specification contains no normative statements about a TCPA subsystem. Page 1. TCPA further teaches that nothing in the TCPA specification is intended to imply the status of any particular data or method for compliance with the TCPA specification. Page 1. TCPA further teaches that the purpose of the specification is to encourage the use of computer platforms for critical purposes. Page 1. The Examiner has not provided any reasons as to why one skilled in the art would modify the specification of TCPA (which teaches that it contains no

normative statements about a TCPA subsystem and is a specification to encourage the use of computer platforms for critical purposes) to have software stored in memory in the customer computer for browsing the web site of the credit card company over the network and to have software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network (missing claim limitations). The Examiner's motivation ("for the purpose [of] improving the security in purchasing products using credit card over the network") does not provide such reasoning.

Why would the reason to modify the specification of TCPA (which teaches that it contains no normative statements about a TCPA subsystem and is a specification to encourage the use of computer platforms for critical purposes) to have software stored in memory in the customer computer for browsing the web site of the credit card company over the network (missing claim limitation) be to improve the security in purchasing products using credit card over the network? What is the rationale connection between improving the security in purchasing products via a credit card over the network (Examiner's motivation) and having software stored in memory in the customer computer for browsing the web site of the credit card company over the network (missing claim limitation)?

Further, why would the reason to modify the specification of TCPA (which teaches that it contains no normative statements about a TCPA subsystem and is a specification to encourage the use of computer platforms for critical purposes) to have software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network (missing claim limitation) be to improve the security in purchasing products using credit card over the network? What is the rationale connection between improving the security in purchasing products via a credit card over the network (Examiner's motivation) and having software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network (missing claim limitation)?

Hence, the Examiner's motivation does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify TCPA to include the missing claim limitations of claim 25. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claim 25. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

      11.   <u>Examiner has not specifically addressed claims 26-27 and therefore has not established a *prima facie* case of obviousness in rejecting claims 26-27.</u>

The Examiner simply states that "claims 26-27 contain similar limitations found in claim 25 above, therefore, are rejected by the same rationale." Office Action (10/19/2006), page 6. Appellant respectfully traverses the assertion that claims 26-27 contain limitations that are similar to claim 25 such that the Examiner has effectively addressed the limitations of claims 26-27. In an obviousness rejection, the Examiner is required to provide a reference or combination of references that teaches or suggests each of the claim limitations in order to establish a *prima facie* case of obviousness. M.P.E.P. §§2142-2143. The Examiner has not met this requirement.

Appellant respectfully asserts that TCPA does not teach or suggest "a memory; code stored in said memory; an adapter which communicates data to and receives data from a certificate server and a credit card application server; a Trusted Platform Module (TPM); a CPU, operatively coupled to said memory, said TPM, and said communications adapter, and which executes code stored in said memory; said CPU when executing said code effective in: creating a TPM identity; obtaining from said communications adapter a first certificate originating from said certificate server; creating a non-migratable key; and transferring a credit card authorization application, said TPM identity, said non-migratable key, and said first certificate to said credit card application server" as recited in claim 26. There are no claim limitations in claim 26 that are similar to claim 25 such that the Examiner has effectively addressed the limitations of claim 26. Therefore, the Examiner has not

presented a *prima facie* case of obviousness in rejecting claim 26, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Appellant respectfully asserts that TCPA does not teach or suggest "an adapter through which data is exchanged with a certificate server and a credit card application server, a Trusted Platform Module (TPM) which creates a TPM identity; a CPU coupled to said adapter and to said TPM and effective in: (1) obtaining from said adapter a first certificate originating from the certificate server; (2) creating a non-migratable key and transferring said non-migratable key, said TPM identity, said first certificate, and a credit card authorization application to the credit card application server" as recited in claim 27. There are no claim limitations in claim 27 that are similar to claim 25 such that the Examiner has effectively addressed the limitations of claim 27. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claim 27, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).
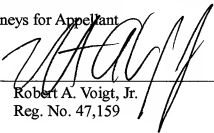
VIII.   <u>CONCLUSION</u>

For the reasons noted above, the rejections of claims 1-27 are in error. Appellant respectfully requests reversal of the rejections and allowance of claims 1-27.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Appellant

By:_____

Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

CLAIMS APPENDIX

1.   A method comprising the steps of:

receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA);

creating a public/private key pair and a third certificate in response to the receiving step; and

sending the public/private key pair and the third certificate to the customer over the network.

2.   The method as recited in claim 1, wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network.

3.   The method as recited in claim 1, wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system.

4.   The method as recited in claim 1, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity.

5.   The method as recited in claim 4, wherein the third certificate is associated with an endorsement key of the TPM.

6.   The method as recited in claim 1, wherein the network is the Internet.

7.   A method comprising the steps of:

creating a TPM identity at a customer's computer system;

obtaining, at the customer's computer system, a first certificate from a first server supporting a CA over a network;

creating, at the customer's computer system, a non-migratable key; and

transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company.

8.   The method as recited in claim 7, further comprising the steps of:

the second server supporting the credit card company creating a public/private key pair and a second certificate in response to the transferring step; and

transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system.

9.   The method as recited in claim 8, wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using a traditional mail service.

10.   The method as recited in claim 8, wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using the network.

11.   The method as recited in claim 8, further comprising the step of:

a customer using the public/private key pair and the second certificate for commercial transactions over the network.

12.   The method as recited in claim 11, wherein the network is the Internet.

13.   The method as recited in claim 7, wherein the creating step further comprises creating a public/private key pair.

14.   The method as recited in claim 13, wherein the step of the customer's computer system obtaining the first certificate from the first server supporting the CA over the network further comprises the steps of:

transferring from the customer's computer system to the first server supporting the CA a public portion of the public/private key pair created when the TPM identity is created and a third certificate associated with an endorsement key of the TPM;

the CA checking an authenticity of the third certificate;

the CA creating a fourth certificate for the TPM identity;

the CA encrypting the fourth certificate;

the CA bundling the encrypted fourth certificate with the public portion of the public/private key pair created when the TPM identity is created to create a first bundle; and

the CA encrypting the first bundle with a public key of the third certificate to create a second bundle.

15.   The method as recited in claim 14, wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system further comprises the steps of:

the TPM decrypting the second bundle with a private portion of the third certificate producing the first bundle; and

the TPM decrypting the first bundle with a private portion of the public/private key pair created when the TPM identity is created.

16.   A computer program product adaptable for storage on a computer readable medium, comprising the program steps of:

receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a

34

second certificate acquired by the computer system from a Certification Authority (CA);

creating a public/private key pair and a third certificate in response to the receiving step; and

sending the public/private key pair and the third certificate to the customer over the network.

17.   The computer program product as recited in claim 16, wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network.

18.   The computer program product as recited in claim 16, wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system.

19.   The computer program product as recited in claim 16, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity.

20.   The computer program product as recited in claim 19, wherein the third certificate is associated with an endorsement key of the TPM.

21.   A computer program product adaptable for storage on a computer readable medium, comprising the program steps of:

creating a TPM identity;

obtaining a first certificate from a CA;

creating a non-migratable key;

contacting a web site supporting a credit card company;

sending to the web site an application for a credit card authorization, the TPM identity, the first certificate, and the non-migratable key; and

receiving from the web site a public/private key pair and a second certificate enabling the credit card authorization.

22.   The computer program product as recited in claim 21, further comprising the program step of:

conducting a commercial transaction over the Internet using the credit card authorization as enabled by the public/private key pair and the second certificate.

23.   The computer program product as recited in claim 21, wherein the non-migratable key is a signing key.

24.   The computer program product as recited in claim 21, wherein the non-migratable key is a storage key.

25.   A system comprising:

a server supporting a web site of a credit card company;

a customer computer including a TPM;

a network linked to the server and the customer computer;

first software stored in memory in the customer computer for requesting the TPM to create a TPM identity;

second software stored in memory in the customer computer for obtaining a first certificate over the network from a CA;

third software stored in memory in the customer computer for creating a non-migratable key;

fourth software stored in memory in the customer computer for browsing the web site of the credit card company over the network;

fifth software stored in memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network;

sixth software stored in memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity, the first certificate, and the non-migratable key;

the web site of the credit card company creating a public/private key pair and a second certificate; and

the web site of the credit card company sending the public/private key pair and the second certificate over the network to the customer computer.

26.   A system comprising:

a memory;

code stored in said memory;

an adapter which communicates data to and receives data from a certificate server and a credit card application server;

a Trusted Platform Module (TPM);

a CPU, operatively coupled to said memory, said TPM, and said communications adapter, and which executes code stored in said memory;

said CPU when executing said code effective in:

creating a TPM identity;

obtaining from said communications adapter a first certificate originating from said certificate server;

creating a non-migratable key; and

transferring a credit card authorization application, said TPM identity, said non-migratable key, and said first certificate to said credit card application server.

27.   Apparatus comprising:

an adapter through which data is exchanged with a certificate server and a credit card application server, a Trusted Platform Module (TPM) which creates a TPM identity; a CPU coupled to said adapter and to said TPM and effective in:

(1) obtaining from said adapter a first certificate originating from the certificate server;

        (2) creating a non-migratable key and transferring said non-migratable key, said TPM identity, said first certificate, and a credit card authorization application to the credit card application server.

EVIDENCE APPENDIX

No evidence was submitted pursuant to §§1.130, 1.131, or 1.132 of 37 C.F.R. or of any other evidence entered by the Examiner and relied upon by Appellant in the Appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings to the current proceeding.